

PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

To:

Commissioner
US Department of Commerce
United States Patent and Trademark
Office, PCT
2011 South Clark Place Room
CP2/5C24
Arlington, VA 22202
ETATS-UNIS D'AMERIQUE
in its capacity as elected Office

Date of mailing (day/month/year) 20 November 2000 (20.11.00)	
International application No. PCT/GB00/01010	Applicant's or agent's file reference A25773 WO
International filing date (day/month/year) 17 March 2000 (17.03.00)	Priority date (day/month/year) 31 March 1999 (31.03.99)
Applicant BROCKBANK, Robert, Grenville et al	

1. The designated Office is hereby notified of its election made:

☒ in the demand filed with the International Preliminary Examining Authority on:21 September 2000 (21.09.00)☐ in a notice effecting later election filed with the International Bureau on:

2. The election
- ☒
- was
-
- ☐
- was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No.: (41-22) 740.14.35	Authorized officer Pascal Piriou Telephone No.: (41-22) 338.83.38
---	---



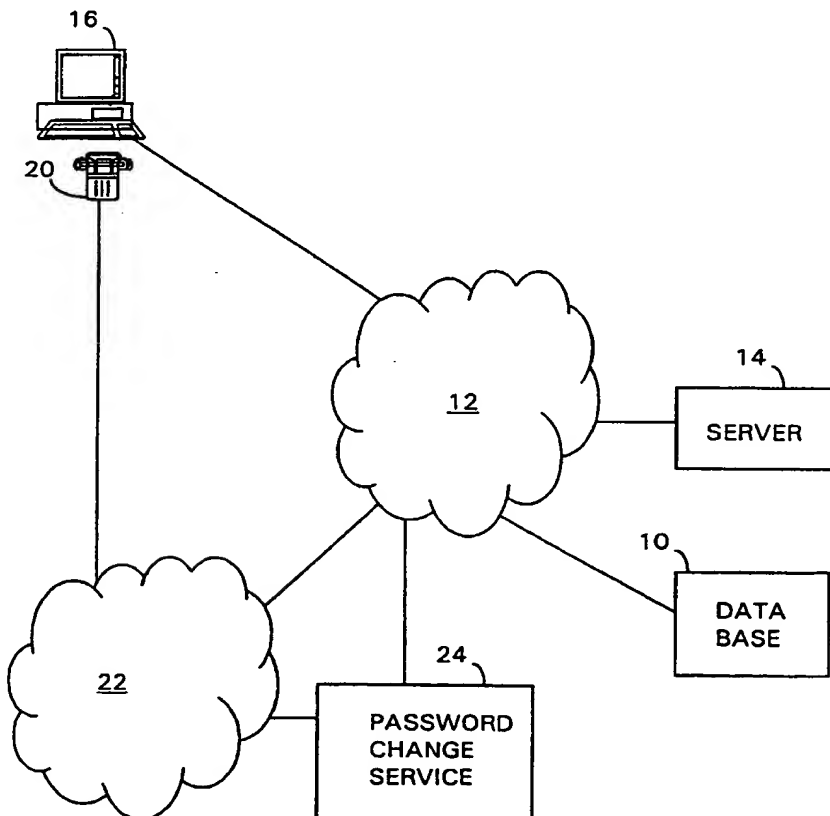
INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁷ : G06F 1/00		A1	(11) International Publication Number: WO 00/58808
			(43) International Publication Date: 5 October 2000 (05.10.00)
(21) International Application Number: PCT/GB00/01010 (22) International Filing Date: 17 March 2000 (17.03.00) (30) Priority Data: 9907430.4 31 March 1999 (31.03.99) GB 99305272.0 2 July 1999 (02.07.99) EP (71) Applicant (for all designated States except US): BRITISH TELECOMMUNICATIONS PUBLIC LIMITED COMPANY [GB/GB]; 81 Newgate Street, London EC1A 7AJ (GB). (72) Inventors; and (75) Inventors/Applicants (for US only): BROCKBANK, Robert, Grenville [GB/GB]; Stellar House, 78 Castle Street, Woodbridge, Suffolk IP12 1HL (GB). EMERSON, Derek, John [GB/GB]; 28 Cedar Avenue, Kesgrave, Ipswich, Suffolk IP5 1EZ (GB). (74) Agent: SEMOS, Robert, Ernest, Vickers; BT Group Legal Services, Intellectual Property Dept., Holborn Centre, 8th floor, 120 Holborn, London EC1N 2TE (GB).		(81) Designated States: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG). Published <i>With international search report.</i>	

(54) Title: **PASSWORD PROTECTION**

(57) Abstract

In password protection access, a nominated telephone number is used as the user identity associated with the protected information. If the user needs to change his password, he makes a call from the nominated telephone to a change password service, which automatically retrieves the calling line identity from the signalling information of the incoming call, prompts for a new password, receives the new password from the user, and records the new password in place of the previous password. There is no involvement of system administration personnel, and no consequent delay while a manual reset of the user's password is effected.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Larvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon		Republic of Korea	PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

PASSWORD PROTECTION

This invention relates to password protection and particularly, but not exclusively, to a method of updating a password by direct user input from a telephone.

In accordance with one aspect of the present invention, there is provided a method of managing password update for a password protected access system having a password store in which each entry comprises a respective network terminal identity store and an associated respective password store, the method comprising the steps of:

making a call to a password change service from a network terminal, retrieving by the password change service from signalling information of the call received thereat the identity of the network terminal from which that call was made; receiving a new password entered at that network terminal;

accessing the password store in accordance with the retrieved network terminal identity to find an entry whose stored network terminal identity matches that retrieved network terminal identity; and

writing the received new password into the associated respective password store of an entry so found.

An advantage of a method of the present invention is the avoidance, and consequent delay, of password resetting procedures performed by system administration personnel.

In accordance with another aspect of the present invention, there is provided a password protected access system comprising means for receiving a call from a network terminal and for retrieving from signalling information of the call the identity of the network terminal from which that call was made, means for receiving from that network terminal information representative of a password, and means for updating the content of a respective password store associated with that network terminal identity by writing said information representative of a password into that associated respective password store.

Specific embodiments of the present invention will now be described by way of example with reference to the drawing in which Figure 1 shows component parts of a password change service of the present invention.

By way of background to the present invention, it is known for password protected access to, for example, a remote database holding a user's personal information, to be performed by user providing a user identity, also called a username or a userID, to identify the particular stored information which the user is requesting access to, and a password. The user identity is commonly a set of letters, often the initials of the user's names, e.g. dje or rgb. The provided password is compared with a password previously provided by the user and stored in association with the user identity, and, if there is a match, the user is granted access.

In this known arrangement, if the user forgets his password, he has to contact the system administrator responsible for the database, provide sufficient proof of his identity, and request a reset of his password. The system administrator has to effect a change of the recorded password to a nominal password, for example "password", and notify the user of that nominal password. The user can thereafter access his information using that nominal password, but for security reasons usually performs a change password procedure to change that nominal password to one which is more secure. In this change password procedure, the user is asked to enter the existing password, then his newly chosen password, and, for confirmation, to enter the new password again.

In the present invention, the user identity is not in the form of the user's initials, but is a nominated network terminal identity, which in this embodiment is a telephone number, and this will usually be the number of the user's home or work telephone. Herein the terms nominated telephone number and nominated telephone are used synonymously and interchangeably.

For normal access, the user calls the password protection system from any telephone, and when prompted for a user identity he enters the nominated telephone number via the keypad, or speaks it if there is an interactive voice response unit (IVR) at the password protection system. The user will then be prompted in the usual manner for entry of his password, which, likewise, he enters via the keypad or the IVR.

If the user has forgotten his password, he makes a call from the telephone corresponding to the nominated number, i.e. the nominated telephone, to a password change service of the password protection system. On receipt at the password protection system of the incoming call from the user, the signalling information is

examined and the content of the calling line identity field (CLI) is retrieved, and the user is prompted to enter a new password, via keypad or the IVR. This new password is then stored in place of the previously stored password in association with the user identity in the form of the retrieved CLI, i.e. the nominated telephone
5 number.

This password change procedure avoids the inefficient use of system administration personnel, the delay to the user when such system administration personnel perform a manual change, and the risk that the user fails to change from the nominal password, which is inherently insecure, to a more secure password.

10 In a specific embodiment shown in Figure 1, the password protected information is a electronic personal telephone or email address book remotely stored on a database 10, accessed via a data network 12, such as the Internet or a corporate intranet, and a server 14.

The user activates a computer 16 at any suitable site, and launches a
15 browser in known manner to access the server 14. He receives from the server 14 an access page having text boxes for the entry of a user identity and a password. Using the keyboard, the user enters the nominated telephone number for the user identity, and the current password. The server 14 performs a comparison of the entered password with the stored password associated with that user identity, and upon a
20 match permits the user access to his address book.

If the user has forgotten his password, or if someone has managed to obtain access to the user's nominated telephone, say his work telephone, and change the password, then the user makes a call from his work telephone 20, via a telephone network, for example a private telephone network 22, to a predetermined destination
25 terminal number at a CTI system 24 operating a change password service.

As shown in the Figure, the change password service is operated by a CTI system 24 which is at a geographically separate location from the server 14. In variants, the CTI system 24 operating a change password service can be local to the server 14, or that function can even be made integral with the server 14.

30 In the present embodiment, the CTI system 24 will send the user's identity (CLI) and new password to the database 10. Thus in this specific embodiment, the CTI system 24 constitutes means for receiving a call from a network terminal and for retrieving from signalling information of the call the identity of the network terminal

from which that call was made, means for receiving from that network terminal information representative of a password, and means for updating a current password stored in association with that network terminal identity by replacing it with said information representative of a password. In a variant, the CTI system 24
5 sends the user's identity (CLI) and new password to the database 10 via the server 14.

The change password service is also responsible for establishing a new user area in the database. A new user makes a call to the change password service, and upon prompting for a telephone number enters a telephone number, and upon
10 prompting for a password the user either enters a password or, if the user chooses not to provide a password at this initial area set up stage, terminates the user area set up procedure in some appropriate manner, e.g. by going on hook or entering "#" on the keypad. This entering of a telephone number by the user constitutes direct provision of a network terminal identity by the user. The change password service
15 now communicates with the database 10 and requests the allocation of a new user area, i.e. a telephone number store and an associated password store, and provides that entered telephone number to the database 10, together with the entered password, if provided by the user at this stage.

If the user enters a password at the password prompt, the database 10 sets
20 a Password Set flag associated with that newly established user area. If the user did not enter a password at the password prompt, the content of the password store in that user area remains filled with null characters, and the Password Set flag remains reset. The establishing of a new user area can alternatively be performed by system administration personnel upon receipt of the required information from a new user
25 via, for example, the postal service. Once a new user area has been established, the user then updates the latest recorded password in his area using the method of the present invention by making a call to the change password service from the nominated telephone. It will be understood that the latest recorded password can be any of: null characters when the user has set up a new area but has not provided a
30 password; or an initially provided password; or the password entered at the latest use of the change password service.

In a variant, the new user area can be set up via the user's computer 16 by downloading a set up page from the server 14, entering the nominated telephone

number and, if required at this stage, a password, in respective text entry boxes, and clicking on a submit button in known manner. This entering of a telephone number by the user constitutes direct provision of a network terminal identity by the user.

In a further variant, since the change password service retrieves a CLI from an incoming call, the user can indicate to the change password service, by entering # on the telephone keypad, that he wishes that CLI to be used as the nominated telephone number. This utilising by the change password service of the CLI in response to a command ("#") from the user constitutes indirect provision of a network terminal identity by the user. The change password service will respond by requesting the user to enter a password. If the user is merely setting up a new user area and intending to defer providing a password, he need not supply a password at this time, and can indicate this by again entering #.

Whereas it is most convenient for the nominated telephone number to be the telephone where the user is most likely to be located when he needs to call the change password service, it need not be so. As an example of a different procedure, a user may nominate the telephone number of a trusted person, e.g. his father, living in a completely different area to where he works, possibly even a different country. The present invention will still work, provided that the calling line identity is delivered. The user now calls his trusted person, gives him a new password and asks him to call the change password service and enter the new password when prompted.

Unless the context clearly requires otherwise, throughout the description and the claims, the words "comprise", "comprising" and the like are to be construed in an inclusive as opposed to an exclusive or exhaustive sense; that is to say, in the sense of "including, but not limited to".

CLAIMS

1. A method of managing password update for a password protected access system having a password store in which each entry comprises a respective network
5 terminal identity store and an associated respective password store, the method comprising the steps of:
 - making a call to a password change service from a network terminal,
 - retrieving by the password change service from signalling information of the call received thereat the identity of the network terminal from which that call was made;
 - 10 receiving a new password entered at that network terminal;
 - accessing the password store in accordance with the retrieved network terminal identity to find an entry whose stored network terminal identity matches that retrieved network terminal identity; and
 - writing the received new password into the associated respective password
15 store of an entry so found.
2. A password protected access system comprising means for receiving a call from a network terminal and for retrieving from signalling information of the call the identity of the network terminal from which that call was made, means for receiving
20 from that network terminal information representative of a password, and means for updating the content of a respective password store associated with that network terminal identity by writing said information representative of a password into that associated respective password store.
- 25 3. A method of managing password update for password protected access, the method being substantially as hereinbefore described with reference to the drawing.
4. A password protected access system substantially as hereinbefore described with reference to the drawing.

1/1

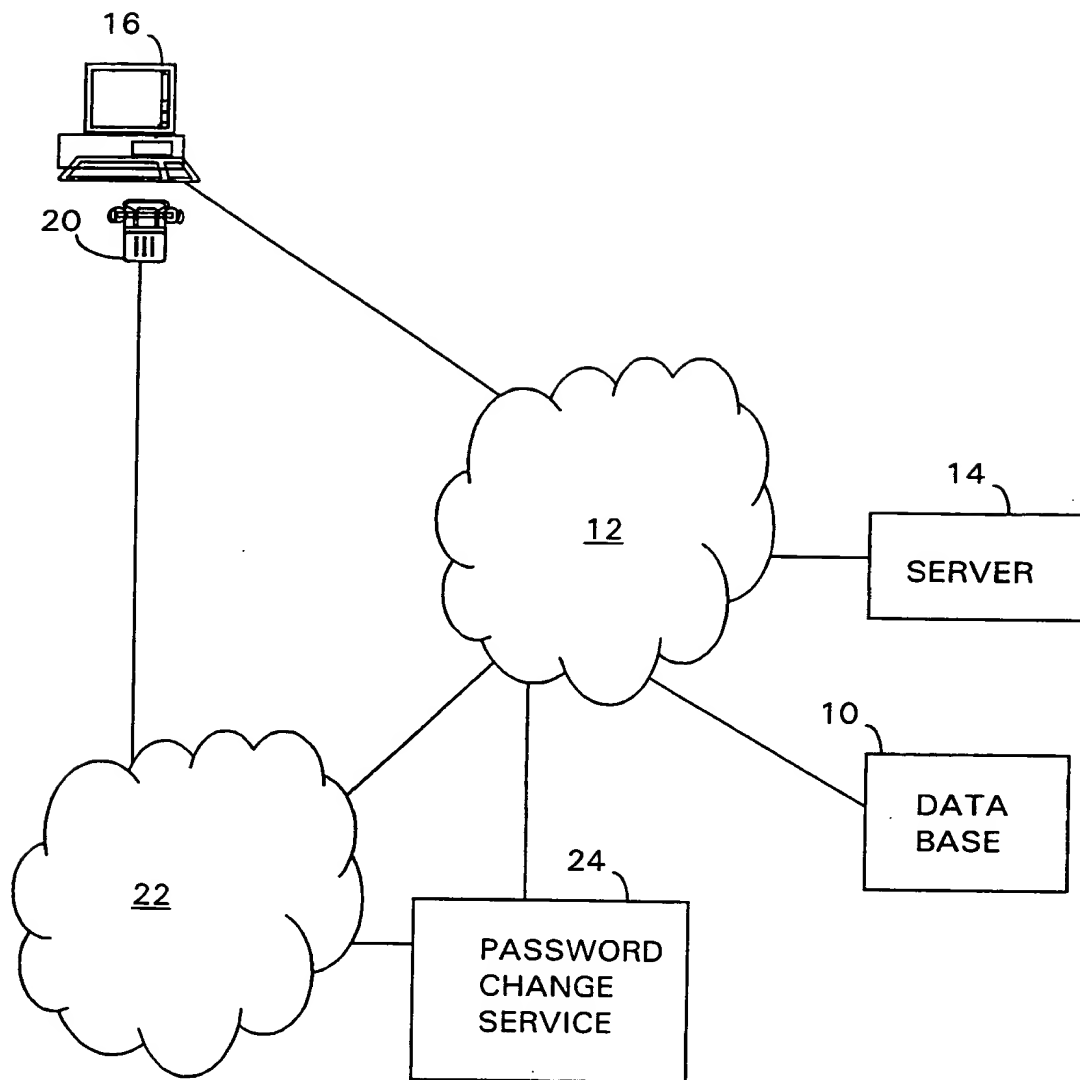


Fig. 1

INTERNATIONAL SEARCH REPORT

Inter. Application No
PCT/GB 00/01010

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 745 924 A (AT & T CORP) 4 December 1996 (1996-12-04) abstract column 5, line 43 -column 6, line 4 column 7, line 42 -column 8, line 3; figures	1-4
X	--- PATENT ABSTRACTS OF JAPAN vol. 1995, no. 08, 29 September 1995 (1995-09-29) & JP 07 129511 A (NIPPON TELEGR & TELEPH CORP), 19 May 1995 (1995-05-19) abstract	1-4
A	--- EP 0 862 104 A (CASIO COMPUTER CO LTD) 2 September 1998 (1998-09-02) abstract; figures --- -/--	1-4

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents:

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the international filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the international filing date but later than the priority date claimed

- *T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- *Z* document member of the same patent family

Date of the actual completion of the international search

20 June 2000

Date of mailing of the international search report

28/06/2000

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Moens, R

INTERNATIONAL SEARCH REPORT

Inter. Application No
PCT/GB 00/01010

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	<p>EP 0 541 435 A (FUJITSU LTD) 12 May 1993 (1993-05-12) abstract</p> <p>-----</p>	1-4

INTERNATIONAL SEARCH REPORT

information on patent family members

Inter: Application No

PCT/GB 00/01010

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0745924 A	04-12-1996	US 5721780 A CA 2172566 A JP 8340331 A	24-02-1998 01-12-1996 24-12-1996
JP 07129511 A	19-05-1995	NONE	
EP 0862104 A	02-09-1998	JP 10243120 A JP 11175477 A CN 1193862 A	11-09-1998 02-07-1999 23-09-1998
EP 0541435 A	12-05-1993	JP 2000620 C JP 5130096 A JP 7012172 B DE 69202682 D DE 69202682 T KR 9605440 B US 5365580 A	20-12-1995 25-05-1993 08-02-1995 29-06-1995 28-09-1995 25-04-1996 15-11-1994

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference A25773 WO	FOR FURTHER ACTION See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. PCT/GB00/01010	International filing date (day/month/year) 17/03/2000	Priority date (day/month/year) 31/03/1999
International Patent Classification (IPC) or national classification and IPC G06F1/00		
Applicant BRITISH TELECOMMUNICATIONS PUBLIC LIMITED COMPANY		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.



2. This REPORT consists of a total of 7 sheets, including this cover sheet.

☒ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of 14 sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☒ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☒ Certain defects in the international application
- VIII ☒ Certain observations on the international application

Date of submission of the demand 21/09/2000	Date of completion of this report 23.07.2001
Name and mailing address of the international preliminary examining authority:  European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Authorized officer Gordon, M Telephone No. +49 89 2399 2901 

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT**

International application No. PCT/GB00/01010

I. Basis of the report

1. With regard to the **elements** of the international application (*Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rules 70.16 and 70.17)*):

Description, pages:

1-10 as received on 09/07/2001 with letter of 09/07/2001

Claims, No.:

1-10 as received on 09/07/2001 with letter of 09/07/2001

Drawings, sheets:

1 as originally filed

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

These elements were available or furnished to this Authority in the following language: , which is:

- ☐ the language of a translation furnished for the purposes of the international search (under Rule 23.1(b)).
- ☐ the language of publication of the international application (under Rule 48.3(b)).
- ☐ the language of a translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

- ☐ contained in the international application in written form.
- ☐ filed together with the international application in computer readable form.
- ☐ furnished subsequently to this Authority in written form.
- ☐ furnished subsequently to this Authority in computer readable form.
- ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
- ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. The amendments have resulted in the cancellation of:

- ☐ the description, pages:
- ☐ the claims, Nos.:

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT**

International application No. PCT/GB00/01010

☐ the drawings, sheets:

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)):

(Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.)

6. Additional observations, if necessary:

III. Non-establishment of opinion with regard to novelty, inventive step and industrial applicability

1. The questions whether the claimed invention appears to be novel, to involve an inventive step (to be non-obvious), or to be industrially applicable have not been examined in respect of:

☐ the entire international application.

☒ claims Nos. 6-10.

because:

☐ the said international application, or the said claims Nos. relate to the following subject matter which does not require an international preliminary examination (*specify*):

☒ the description, claims or drawings (*indicate particular elements below*) or said claims Nos. 6-10 are so unclear that no meaningful opinion could be formed (*specify*):
see separate sheet

☐ the claims, or said claims Nos. are so inadequately supported by the description that no meaningful opinion could be formed.

☐ no international search report has been established for the said claims Nos. .

2. A meaningful international preliminary examination cannot be carried out due to the failure of the nucleotide and/or amino acid sequence listing to comply with the standard provided for in Annex C of the Administrative Instructions:

☐ the written form has not been furnished or does not comply with the standard.

☐ the computer readable form has not been furnished or does not comply with the standard.

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)

Yes: Claims 1-5

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No. PCT/GB00/01010

	No:	Claims	
Inventive step (IS)	Yes:	Claims	1-4
	No:	Claims	5
Industrial applicability (IA)	Yes:	Claims	1-5
	No:	Claims	

2. Citations and explanations
see separate sheet

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:
see separate sheet

VIII. Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:
see separate sheet

Re Item III

Non-establishment of opinion with regard to novelty, inventive step and industrial applicability

1. Dependent claims 6 to 10 contain no additional limiting features beyond a mere reference to the single drawing figure. According to Rule 6.2(a) PCT, claims should not contain such references except where absolutely necessary, which is not the case here. Claims 6 to 10 thus provide no additional examinable material and so should have been omitted.

Re Item V

Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Reference is made to the following documents:

D1: EP-A-0 862 104 (Casio Computer Co Ltd) 2 September 1998 (1998-09-02)
D2: EP-A-0 541 435 (Fujitsu Ltd) 12 May 1993 (1993-05-12)
D3: Patent Abstracts of Japan vol. 1995, no. 08, 29 September 1995 (1995-09-29) & JP 07 129511 A (Nippon Telegraph & Telephone Corp), 19 May 1995 (1995-05-19)
D4: EP-A-0 745 924 (AT & T Corp) 4 December 1996 (1996-12-04)
2. The subject-matter of claims 1 to 4 is distinguished from the cited prior art disclosures by the feature, common to each claim, that the password update service retrieves from signalling information of the received call the identity of the network terminal from which the call is made and accesses the password store in accordance with the retrieved identity. Since this feature is neither known from, nor suggested by, the cited prior art, the claims exhibit novelty and inventive step.
3. Independent claim 5 does not contain the distinguishing feature referred to above. Instead it merely defines the step of requesting the user to enter his nominated terminal identity and password. According to the description at page 3, lines 3 to 4, the nominated terminal identity merely fulfills the function of a user identity.

- 3.1 The prior art is replete with examples of a user supplying a user identity of one sort or another, and this UID being compared against a stored value. Claim 5 gives no indication as to why, within the scope of the activities defined in that claim, the use of a nominated terminal identity as a user identity, to be supplied manually by the user, would introduce any new or surprising technical effect when compared to the use of any other kind of identity as a user identity, when supplied manually by the user. Thus the use in claim 5 of a nominated terminal identity as a user identity does not confer inventive step.
- 3.2 For the rest, claim 5 merely defines completely ordinary activities which are either known or obvious, from D3 for example. In D3, as acknowledged by the Applicant, "a person makes a telephone call to the system and provides his identifier IDn (which equates to the user identity in claim 5) and his old PIN Pn1 (which equates to the password in claim 5). A part 2 receives this data (IDn and PN1) and authenticates (confirms) the person from the corresponding stored data for that person". This is what is defined in claim 5.
- 3.3 The fact that, in D3, the person makes the telephone call for the purpose of changing his PIN, the system is a PIN alteration system, and the part 2 is a PIN alteration information temporary storing part, merely relates to the intended purpose in D3 of the authenticating procedure (i.e. to permit changing a password). This fact does not make the initial authenticating procedure in D3 any less relevant to claim 5 from the standpoint of obviousness.

Re Item VII

Certain defects in the international application

1. The amendments filed with the letter dated 9.7.2001 introduce subject-matter which extends beyond the content of the application as filed, contrary to Article 34(2)(b) PCT. The amendments concerned are the following:
- 1.1 In claim 1, lines 14 to 15, claim 2, lines 31 to 32, claim 3, line 18 and claim 4, line 4 the phrase "playing an announcement to the caller". In the originally filed application documents only the terms "prompted" (description, page 3, line 2) and

- "requesting" (description, page 5, line 10) are used.
- 1.2 In claim 3, line 5 (i.e. the first line) the term "registering". In the originally filed application documents the term "establishing" is used (description, page 4, line 7).
 - 1.3 In claim 3, lines 9, 10 and 20, and in claim 4 at corresponding positions the term "management". There is no reference whatsoever in the originally filed application documents to this activity as such.
 - 1.4 In the description at page 1, lines 5 to 6 the sentence relating to synonymous use of the terms "updating" and "changing".
 - 1.5 In the description at page 3, lines 6 to 10 the sentence relating to an advantage.
 - 1.6 In the description at page 7, lines 25 to 26 the phrase "also ... management service". There is no reference whatsoever in the originally filed application documents to this activity as such.
 - 1.7 The entire paragraph in the description at page 9, lines 10 to 28.
 2. The features of the claims are not provided with reference signs placed in parentheses (Rule 6.2(b) PCT).
 3. The description does not conform to an acceptable set of claims as required by Rule 5.1(a)(iii)PCT.

Re Item VIII

Certain observations on the international application

1. Claims 1 to 4 are unclear since each defines an "entry" in the password store as itself comprising a "store", for example "a respective network terminal identity store" and "an associated respective password store". An entry in a store is actually an item of data and not a store per se. The word "store" should have been omitted from these terms. By contrast, claim 5 defines the terms correctly.

PASSWORD PROTECTION

This invention relates to password protection and particularly, but not exclusively, to a method of updating a password by direct user input from a
5 telephone.

In accordance with one aspect of the present invention, there is provided a method of managing password update for a password protected access system having a password store in which each entry comprises a respective network terminal identity store and an associated respective password store, the method comprising
10 the steps of:

making a call to a password change service from a network terminal, retrieving by the password change service from signalling information of the call received thereat the identity of the network terminal from which that call was made; receiving a new password entered at that network terminal;

15 accessing the password store in accordance with the retrieved network terminal identity to find an entry whose stored network terminal identity matches that retrieved network terminal identity; and

writing the received new password into the associated respective password store of an entry so found.

20 An advantage of a method of the present invention is the avoidance, and consequent delay, of password resetting procedures performed by system administration personnel.

In accordance with another aspect of the present invention, there is provided a password protected access system comprising means for receiving a call from a
25 network terminal and for retrieving from signalling information of the call the identity of the network terminal from which that call was made, means for receiving from that network terminal information representative of a password, and means for updating the content of a respective password store associated with that network terminal identity by writing said information representative of a password into that
30 associated respective password store.

Specific embodiments of the present invention will now be described by way of example with reference to the drawing in which Figure 1 shows component parts of a password change service of the present invention.

By way of background to the present invention, it is known for password protected access to, for example, a remote database holding a user's personal information, to be performed by user providing a user identity, also called a username or a userID, to identify the particular stored information which the user is requesting
5 access to, and a password. The user identity is commonly a set of letters, often the initials of the user's names, e.g. dje or rgb. The provided password is compared with a password previously provided by the user and stored in association with the user identity, and, if there is a match, the user is granted access.

In this known arrangement, if the user forgets his password, he has to
10 contact the system administrator responsible for the database, provide sufficient proof of his identity, and request a reset of his password. The system administrator has to effect a change of the recorded password to a nominal password, for example "password", and notify the user of that nominal password. The user can thereafter access his information using that nominal password, but for security reasons usually
15 performs a change password procedure to change that nominal password to one which is more secure. In this change password procedure, the user is asked to enter the existing password, then his newly chosen password, and, for confirmation, to enter the new password again.

In the present invention, the user identity is not in the form of the user's
20 initials, but is a nominated network terminal identity, which in this embodiment is a telephone number, and this will usually be the number of the user's home or work telephone. Herein the terms nominated telephone number and nominated telephone are used synonymously and interchangeably.

For normal access, the user calls the password protection system from any
25 telephone, and when prompted for a user identity he enters the nominated telephone number via the keypad, or speaks it if there is an interactive voice response unit (IVR) at the password protection system. The user will then be prompted in the usual manner for entry of his password, which, likewise, he enters via the keypad or the IVR.

30 If the user has forgotten his password, he makes a call from the telephone corresponding to the nominated number, i.e. the nominated telephone, to a password change service of the password protection system. On receipt at the password protection system of the incoming call from the user, the signalling information is

examined and the content of the calling line identity field (CLI) is retrieved, and the user is prompted to enter a new password, via keypad or the IVR. This new password is then stored in place of the previously stored password in association with the user identity in the form of the retrieved CLI, i.e. the nominated telephone
5 number.

This password change procedure avoids the inefficient use of system administration personnel, the delay to the user when such system administration personnel perform a manual change, and the risk that the user fails to change from the nominal password, which is inherently insecure, to a more secure password.

10 In a specific embodiment shown in Figure 1, the password protected information is a electronic personal telephone or email address book remotely stored on a database 10, accessed via a data network 12, such as the Internet or a corporate intranet, and a server 14.

The user activates a computer 16 at any suitable site, and launches a
15 browser in known manner to access the server 14. He receives from the server 14 an access page having text boxes for the entry of a user identity and a password. Using the keyboard, the user enters the nominated telephone number for the user identity, and the current password. The server 14 performs a comparison of the entered password with the stored password associated with that user identity, and upon a
20 match permits the user access to his address book.

If the user has forgotten his password, or if someone has managed to obtain access to the user's nominated telephone, say his work telephone, and change the password, then the user makes a call from his work telephone 20, via a telephone network, for example a private telephone network 22, to a predetermined destination
25 terminal number at a CTI system 24 operating a change password service.

As shown in the Figure, the change password service is operated by a CTI system 24 which is at a geographically separate location from the server 14. In variants, the CTI system 24 operating a change password service can be local to the server 14, or that function can even be made integral with the server 14.

30 In the present embodiment, the CTI system 24 will send the user's identity (CLI) and new password to the database 10. Thus in this specific embodiment, the CTI system 24 constitutes means for receiving a call from a network terminal and for retrieving from signalling information of the call the identity of the network terminal

from which that call was made, means for receiving from that network terminal information representative of a password, and means for updating a current password stored in association with that network terminal identity by replacing it with said information representative of a password. In a variant, the CTI system 24
5 sends the user's identity (CLI) and new password to the database 10 via the server 14.

The change password service is also responsible for establishing a new user area in the database. A new user makes a call to the change password service, and upon prompting for a telephone number enters a telephone number, and upon
10 prompting for a password the user either enters a password or, if the user chooses not to provide a password at this initial area set up stage, terminates the user area set up procedure in some appropriate manner, e.g. by going on hook or entering "#" on the keypad. This entering of a telephone number by the user constitutes direct provision of a network terminal identity by the user. The change password service
15 now communicates with the database 10 and requests the allocation of a new user area, i.e. a telephone number store and an associated password store, and provides that entered telephone number to the database 10, together with the entered password, if provided by the user at this stage.

If the user enters a password at the password prompt, the database 10 sets
20 a Password Set flag associated with that newly established user area. If the user did not enter a password at the password prompt, the content of the password store in that user area remains filled with null characters, and the Password Set flag remains reset. The establishing of a new user area can alternatively be performed by system administration personnel upon receipt of the required information from a new user
25 via, for example, the postal service. Once a new user area has been established, the user then updates the latest recorded password in his area using the method of the present invention by making a call to the change password service from the nominated telephone. It will be understood that the latest recorded password can be any of: null characters when the user has set up a new area but has not provided a
30 password; or an initially provided password; or the password entered at the latest use of the change password service.

In a variant, the new user area can be set up via the user's computer 16 by downloading a set up page from the server 14, entering the nominated telephone

number and, if required at this stage, a password, in respective text entry boxes, and clicking on a submit button in known manner. This entering of a telephone number by the user constitutes direct provision of a network terminal identity by the user.

In a further variant, since the change password service retrieves a CLI from
5 an incoming call, the user can indicate to the change password service, by entering # on the telephone keypad, that he wishes that CLI to be used as the nominated telephone number. This utilising by the change password service of the CLI in response to a command ("#") from the user constitutes indirect provision of a network terminal identity by the user. The change password service will respond by
10 requesting the user to enter a password. If the user is merely setting up a new user area and intending to defer providing a password, he need not supply a password at this time, and can indicate this by again entering #.

Whereas it is most convenient for the nominated telephone number to be the telephone where the user is most likely to be located when he needs to call the
15 change password service, it need not be so. As an example of a different procedure, a user may nominate the telephone number of a trusted person, e.g. his father, living in a completely different area to where he works, possibly even a different country. The present invention will still work, provided that the calling line identity is delivered. The user now calls his trusted person, gives him a new password and asks
20 him to call the change password service and enter the new password when prompted.

Unless the context clearly requires otherwise, throughout the description and the claims, the words "comprise", "comprising" and the like are to be construed in an inclusive as opposed to an exclusive or exhaustive sense; that is to say, in the sense
25 of "including, but not limited to".

CLAIMS

1. A method of managing password update for a password protected access system having a password store in which each entry comprises a respective network
5 terminal identity store and an associated respective password store, the method comprising the steps of:
making a call to a password change service from a network terminal,
retrieving by the password change service from signalling information of the call received thereat the identity of the network terminal from which that call was made;
10 receiving a new password entered at that network terminal;
accessing the password store in accordance with the retrieved network terminal identity to find an entry whose stored network terminal identity matches that retrieved network terminal identity; and
writing the received new password into the associated respective password
15 store of an entry so found.
2. A password protected access system comprising means for receiving a call from a network terminal and for retrieving from signalling information of the call the identity of the network terminal from which that call was made, means for receiving
20 from that network terminal information representative of a password, and means for updating the content of a respective password store associated with that network terminal identity by writing said information representative of a password into that associated respective password store.
- 25 3. A method of managing password update for password protected access, the method being substantially as hereinbefore described with reference to the drawing.
4. A password protected access system substantially as hereinbefore described with reference to the drawing.

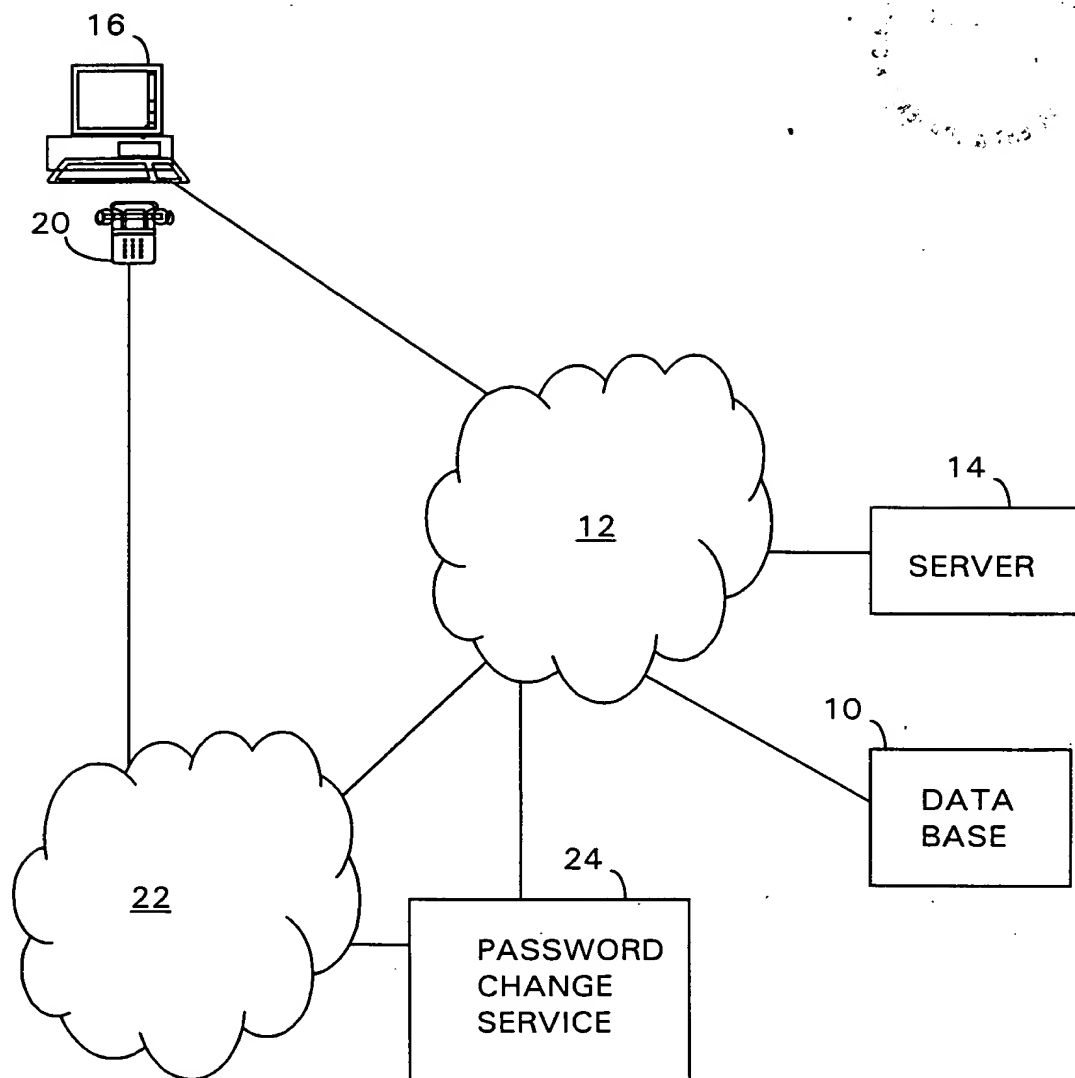
ABSTRACT

PASSWORD PROTECTION

In password protection access, a nominated telephone number is used as the user identity associated with the protected information. If the user needs to change
5 his password, he makes a call from the nominated telephone to a change password service, which automatically retrieves the calling line identity from the signalling information of the incoming call, prompts for a new password, receives the new password from the user, and records the new password in place of the previous password. There is no involvement of system administration personnel, and no
10 consequent delay while a manual reset of the user's password is effected.

Figure (1)

15

**Fig. 1**

1
PASSWORD PROTECTION

This invention relates to password protection and particularly, but not exclusively, to a method of updating a password by direct user input from a telephone. In this application, the terms updating and changing are used synonymously.

European Patent Application EP 0 862 104 A (Casio Computer Co., Ltd.) discloses an authentication system in which a user's terminal device stores the user's username and his password, and for each access attempt authentication is based upon the username and password read out of the store in the terminal device and sent to the authentication server. This avoids the need for the user to remember his username and password. There is also disclosed the use of the telephone number of the terminal device as the user's username, and obtaining this telephone number from the incoming access attempt call. Thus, in this case only the user's password is required to be read from the store in the terminal device and sent to the authentication server.

European Patent Application EP 0 541 435 A (Fujitsu Limited) discloses an authentication system in which a caller provides a username and a password, which are checked. If they match an existing entry, the telephone number from which that current access attempt is being made is obtained from the incoming call, stored for use with the next access attempt for that username, and compared with the corresponding telephone number stored for the previous access attempt. If there is no match, a warning message is played and the caller is requested to enter a second password. This system helps to prevent fraudulent use of a person's username and password from a telephone different from the one that the person normally uses.

European Patent Application EP 0 745 924 A (AT&T) discloses a method of authenticating user terminal access to a service provider by means of a service bureau. The service bureau sets up a new user terminal for password authenticated access by encrypting the calling line identity (CLI) associated with that user's terminal, which the service bureau obtains from a network-based automatic number identification (ANI) unit, and sending the encrypted CLI to the user's terminal for storage as a password. When the user desires access to the service provider, he makes a call from his user terminal to the service bureau, which encrypts the CLI of

09-07-2001

GB00010

2

that call, automatically retrieves the password stored in the user's terminal and, upon finding a match between the retrieved password and the newly encrypted CLI, permits access to the service provider.

The service bureau is programmed for automatically changing the password stored in the user's terminal. This change is effected following normal authentication of a user terminal by the service bureau re-encrypting the CLI using a different encryption key, and sending the newly-encrypted CLI to the user's terminal to be stored for use instead of the previously stored password.

Japanese Patent Application JP 07 129511 A (Nippon Telegraph and Telephone Corporation) discloses a method of changing a user's password in which the user contacts the password change service (PCS) from a telephone previously designated to the PCS, gives his user ID, and then enters a new password. The PCS looks up the user's ID in its database and retrieves the designated telephone number associated with that user's ID. The PCS makes a call to that designated telephone number and requests the user to enter the password again. The PCS compares this second entered password with the first entered password, and upon a match writes the password to its database in association with that user's ID.

In accordance with a first aspect of the present invention, there is provided a method of password update for a password protected access system having a password store in which each entry is constituted by a respective network terminal identity store and an associated respective password store, the method comprising the steps of:

- receiving at a password update service a call from a network terminal;
- retrieving by the password update service from signalling information of that received call the identity of the network terminal from which that call was made;
- accessing the password store in accordance with the retrieved network terminal identity; and
- characterised by the steps of:
 - upon locating an entry whose stored network terminal identity matches that retrieved network terminal identity, playing an announcement to the caller requesting the entry of a password at that network terminal; and

09.07.2001

GB00001C

3

upon receipt at the password update service of a password entered in response to that request, writing that received password into the associated respective password store of the located entry.

An advantage of a method of the present invention is the avoidance of
5 manual password resetting procedures performed by system administration personnel. Another advantage is that it is a quick and simple one-step password entry procedure that does not involve any call-back to a designated number, and thus avoids any problems that would arise should that designated number have special call handling set, such as divert, which would result in that call not being
10 delivered to the designated number.

In accordance with a second aspect of the present invention, there is provided a password protected access system having a password store in which each entry is constituted by a respective network terminal identity store and an associated respective password store, and including a password update system
15 comprising:

means for receiving a call from a network terminal;

means for retrieving from signalling information of that received call the identity of the network terminal from which that call was made; and

means for accessing the password store in accordance with the retrieved
20 network terminal identity; and
characterised by:

means responsive to a successful location of an entry whose stored network terminal identity matches that retrieved network terminal identity, for playing an announcement to the caller requesting the entry of a password at that network
25 terminal; and

means responsive to receipt of a password entered in response to that request, for writing that received password into the associated respective password store of the located entry.

In accordance with a third aspect of the present invention, there is provided
30 a method of registering a new user of a password protected access system having a password store in which each entry is constituted by a respective network terminal identity store and an associated respective password store, the method comprising the steps of:

Empf.zeit:09/07/2001 18:17

Empf.nr.:156 P.013

AMENDED SHEET

receiving at a password management service a call from a network terminal;
retrieving by the password management service from signalling information
of that received call the identity of the network terminal from which that call was
made;

- 5 accessing the password store in accordance with the retrieved network
terminal identity;

 upon failure to locate an entry whose stored network terminal identity
matches that retrieved network terminal identity, making a new entry in respect of
that retrieved network terminal identity;

- 10 playing an announcement to the caller requesting the entry of a password at
that network terminal; and

 upon receipt at the password management service of a password entered in
response to that request, writing that received password into the associated
respective password store of the newly made entry.

- 15 In accordance with a fourth aspect of the present invention, there is
provided a password protected access system having a password store in which
each entry is constituted by a respective network terminal identity store and an
associated respective password store, and including a password management
system comprising;

- 20 means for receiving a call from a network terminal;
 means for retrieving from signalling information of that received call the
identity of the network terminal from which that call was made; and
 means for accessing the password store in accordance with the retrieved
network terminal identity; and

- 25 characterised by:

 means responsive to an unsuccessful location of an entry whose stored
network terminal identity matches that retrieved network terminal identity, for
making a new entry in respect of that retrieved network terminal identity and for
triggering the playing of an announcement to the caller requesting the entry of a

- 30 password at that network terminal; and

 means responsive to receipt of a password entered in response to that
request, for writing that received password into the associated respective password
store of the newly made entry.

In accordance with a fifth aspect of the present invention, there is provided a method of user authentication in a password protected access system having a password store in which each entry is constituted by a respective user-nominated network terminal identity and an associated respective password, the method comprising the steps of:

in response to receipt at the password protected access system of a call from a calling user at a network terminal, requesting the calling user to enter at that network terminal his nominated terminal identity and password;

receiving the entered terminal identity and password;

accessing the password store in accordance with the received entered terminal identity; and

upon locating an entry whose stored network terminal identity and associated password match the received entered terminal identity and password, authenticating that calling user.

Specific embodiments of the present invention will now be described by way of example with reference to the drawing in which Figure 1 shows component parts of a password change service of the present invention.

In accordance with the present invention, it is known for password protected access to, for example, a remote database holding a user's personal information, to be performed by user providing a user identity (user ID or userID), also called a username, to identify the particular stored information which the user is requesting access to, and a password. The user identity is commonly a set of letters, often the initials of the user's names, e.g. dje or rgb. The provided password is compared with a password previously provided by the user and stored in association with the user identity, and, if there is a match, the user is granted access.

In this known arrangement, if the user forgets his password, he has to contact the system administrator responsible for the database, provide sufficient proof of his identity, and request a reset of his password. The system administrator has to effect a change of the recorded password to a nominal password, for example "password", and notify the user of that nominal password. The user can thereafter access his information using that nominal password, but for security reasons usually performs a change password procedure to change that nominal password to one which is more secure. In this change password procedure, the user is asked to enter

the existing password, then his newly chosen password, and, for confirmation, to enter the new password again.

In the present invention, the user identity is not in the form of the user's initials, but is a nominated network terminal identity, which in this embodiment is a
5 telephone number, and this will usually be the number of the user's home or work telephone. Herein the terms nominated telephone number and nominated telephone are used synonymously and interchangeably.

For normal access, the user calls the password protection system from any telephone, and when prompted for a user identity he enters the nominated telephone
10 number via the keypad, or speaks it if there is an interactive voice response unit (IVR) at the password protection system. The user will then be prompted in the usual manner for entry of his password, which, likewise, he enters via the keypad or the IVR.

If the user has forgotten his password, he makes a call from the telephone
15 corresponding to the nominated number, i.e. the nominated telephone, to a password change service of the password protection system. On receipt at the password protection system of the incoming call from the user, the signalling information is examined and the content of the calling line identity field (CLI) is retrieved, and the user is prompted to enter a new password, via keypad or the IVR.
20 This new password is then stored in place of the previously stored password in association with the user identity in the form of the retrieved CLI, i.e. the nominated telephone number.

This password change procedure avoids the inefficient use of system administration personnel, the delay to the user when such system administration
25 personnel perform a manual change, and the risk that the user fails to change from the nominal password, which is inherently insecure, to a more secure password.

In a specific embodiment shown in Figure 1, the password protected information is a electronic personal telephone or email address book remotely stored on a database 10, accessed via a data network 12, such as the Internet or a
30 corporate intranet, and a server 14.

The user activates a computer 16 at any suitable site, and launches a browser in known manner to access the server 14. He receives from the server 14 an access page having text boxes for the entry of a user identity and a password.

09-07-2001

G50001

7

Using the keyboard, the user enters the nominated telephone number for the user identity, and the current password. The server 14 performs a comparison of the entered password with the stored password associated with that user identity, and upon a match permits the user access to his address book.

5 If the user has forgotten his password, or if someone has managed to obtain access to the user's nominated telephone, say his work telephone 20, and change the password, then the user makes a call from his nominated telephone 20, via a telephone network, for example a private telephone network 22, to a predetermined destination terminal number at a CTI system 24 operating a change password
10 service.

As shown in the Figure, the change password service is operated by a CTI system 24 which is at a geographically separate location from the server 14. In variants, the CTI system 24 operating a change password service can be local to the server 14, or that function can even be made integral with the server 14.

15 In the present embodiment, the CTI system 24 will send the user's identity (CLI) and new password to the database 10. Thus in this specific embodiment, the CTI system 24 constitutes means for receiving a call from a network terminal and for
20 information representative of a password, and means for updating a current password stored in association with that network terminal identity by replacing it with said information representative of a password. In a variant, the CTI system 24 sends the user's identity (CLI) and new password to the database 10 via the server 14.

25 The change password service, also referred to in this respect as a password management service, is also responsible for establishing a new user area in the database. A new user makes a call to the change password service, and upon prompting for a telephone number enters a telephone number, and upon prompting for a password the user either enters a password or, if the user chooses not to
30 provide a password at this initial area set up stage, terminates the user area set up procedure in some appropriate manner, e.g. by going on hook or entering "#" on the keypad. This entering of a telephone number by the user constitutes direct provision of a network terminal identity by the user. The change password service now

Empf.zeit:09/07/2001 18:19

Empf.nr.:156 P.017

AMENDED SHEET

communicates with the database 10 and requests the allocation of a new user area, i.e. a telephone number store and an associated password store, and provides that entered telephone number to the database 10, together with the entered password, if provided by the user at this stage.

- 5 If the user enters a password at the password prompt, the database 10 sets a Password Set flag associated with that newly established user area. If the user did not enter a password at the password prompt, the content of the password store in that user area remains filled with null characters, and the Password Set flag remains reset. The establishing of a new user area can alternatively be performed by system
- 10 administration personnel upon receipt of the required information from a new user via, for example, the postal service. Once a new user area has been established, the user then updates the latest recorded password in his area using the method of the present invention by making a call to the change password service from the nominated telephone. It will be understood that the latest recorded password can be
- 15 any of: null characters when the user has set up a new area but has not provided a password; or an initially provided password; or the password entered at the latest use of the change password service.

- A user area can be set up via the user's computer 16 by downloading a set up page from the server 14, entering the nominated telephone
- 20 number and, if required at this stage, a password, in respective text entry boxes, and clicking on a submit button in known manner. This entering of a telephone number by the user constitutes direct provision of a network terminal identity by the user.

- In a further variant, since the change password service retrieves a CLI from
- 25 an incoming call, the user can indicate to the change password service, by entering # on the telephone keypad, that he wishes that CLI to be used as the nominated telephone number. This utilising by the change password service of the CLI in response to a command ("#") from the user constitutes indirect provision of a network terminal identity by the user. The change password service will respond by
- 30 requesting the user to enter a password. If the user is merely setting up a new user area and intending to defer providing a password, he need not supply a password at this time, and can indicate this by again entering #.

09-07-2001

GB0001

9

Whereas it is most convenient for the nominated telephone number to be the telephone where the user is most likely to be located when he needs to call the change password service, it need not be so. As an example of a different procedure, a user may nominate the telephone number of a trusted person, e.g. his father, living in a completely different area to where he works, possibly even a different country. The present invention will still work, provided that the calling line identity is delivered. The user now calls his trusted person, gives him a new password and asks him to call the change password service and enter the new password when prompted.

It will now be appreciated that the present invention is concerned with a password change facility in a password protected access for human users, where those users have user identities in the form of network terminal identity (also referred to as a network address). When a user desires access to a required target, e.g. a remote database such as mentioned above, he dials the normal access number for the protection system from any terminal in the network, and provides to the protection system his user identity and password by voice or key input. The protection system uses that provided identity to locate the user's entry and checks the provided password against the stored password. The user decides when he wants to change his password, and dials the special number for the password change service of the protection system. It is this change service that obtains the CLI of the call and upon receipt of the new password entered by the user immediately stores that newly received password in association with that CLI. The procedure of the present invention is easy and quick, avoids any need to use known update procedures, and whenever the user wishes to update his password, whether because he has forgotten it, or because he thinks that its security has been compromised and he wishes to update it for security reasons, or because he thinks that he might have entered his intended new password incorrectly, or whatever, the user only has to repeat the simple method of the present invention.

The present invention distinguishes from the abovementioned AT&T disclosure which is not concerned with human user authentication, but with authentication of an actual terminal equipment by ensuring that the terminal equipment is attached to the network termination corresponding with its original registration. The AT&T authentication system prevents a terminal equipment from

being taken to a different network termination, i.e. telephone line; but it does not provide any protection against a different human user activating the terminal equipment; it does not require the user to provide any personal identity, but merely encrypts the number provided by the network ANI equipment, i.e. the CLI; and it
5 requires the terminal equipment to store that encrypted CLI as a password retrievable from the terminal equipment upon command by the authentication system. Furthermore, it is the authentication system, and not the user, that decides when to replace the stored encrypted CLI in the terminal equipment, that decides the new encryption key, that generates the replacement password rather than receiving the
10 replacement password from a user.

The present invention distinguishes from the abovementioned Casio Computer Co. disclosure which is concerned with capturing a user's originally submitted password, storing it with his username within his terminal device, and instead of using a step of requesting the user to enter his password and username, reads out
15 the stored password and username. In this way, there is no username or password entered by the user at each access attempt, and therefore no possibility of the user forgetting his details and having to contact authentication personnel for password reset (update).

The present invention distinguishes from the abovementioned Nippon Telegraph and Telephone Corporation disclosure which is concerned with authenticating a password update attempt by a combination of dialback security, i.e. making contact with the user by calling him back on a telephone number known to be secure, and requesting a second entry of the new password.

Unless the context clearly requires otherwise, throughout the description and
25 the claims, the words "comprise", "comprising" and the like are to be construed in an inclusive as opposed to an exclusive or exhaustive sense; that is to say, in the sense of "including, but not limited to".

CLAIMS

1. A method of password update for a password protected access system having a password store in which each entry is constituted by a respective network terminal identity store and an associated respective password store, the method comprising the steps of:
 - receiving at a password update service a call from a network terminal;
 - retrieving by the password update service from signalling information of that received call the identity of the network terminal from which that call was made;
 - 10 accessing the password store in accordance with the retrieved network terminal identity; andcharacterised by the steps of:
 - upon locating an entry whose stored network terminal identity matches that retrieved network terminal identity, playing an announcement to the caller requesting
 - 15 the entry of a password at that network terminal; and
 - upon receipt at the password update service of a password entered in response to that request, writing that received password into the associated respective password store of the located entry.
- 20 2. A password protected access system having a password store in which each entry is constituted by a respective network terminal identity store and an associated respective password store, and including a password update system comprising:
 - means for receiving a call from a network terminal;
 - 25 means for retrieving from signalling information of that received call the identity of the network terminal from which that call was made; and
 - means for accessing the password store in accordance with the retrieved network terminal identity; andcharacterised by:
 - 30 means responsive to a successful location of an entry whose stored network terminal identity matches that retrieved network terminal identity, for playing an announcement to the caller requesting the entry of a password at that network terminal; and

09-07-2001

G500016

12

means responsive to receipt of a password entered in response to that request, for writing that received password into the associated respective password store of the located entry.

- 5 3. A method of registering a new user of a password protected access system having a password store in which each entry is constituted by a respective network terminal identity store and an associated respective password store, the method comprising the steps of:

receiving at a password management service a call from a network terminal;
10 retrieving by the password management service from signalling information of that received call the identity of the network terminal from which that call was made;

accessing the password store in accordance with the retrieved network terminal identity;

15 upon failure to locate an entry whose stored network terminal identity matches that retrieved network terminal identity, making a new entry in respect of that network terminal identity;

playing an announcement to the caller requesting the entry of a password at that network terminal; and

20 upon receipt at the password management service of a password entered in response to that request, writing that received password into the associated respective password store of the newly made entry.

4. A password protected access system having a password store in which
25 each entry is constituted by a respective network terminal identity store and an associated respective password store, and including a password management system comprising:

means for receiving a call from a network terminal;

means for retrieving from signalling information of that received call the
30 identity of the network terminal from which that call was made; and

means for accessing the password store in accordance with the retrieved network terminal identity; and
characterised by:

Empf.zeit:09/07/2001 18:20

Empf.nr.:156 P.022

AMENDED SHEET

means responsive to an unsuccessful location of an entry whose stored network terminal identity matches that retrieved network terminal identity, for making a new entry in respect of that retrieved network terminal identity and for triggering the playing of an announcement to the caller requesting the entry of a
5 password at that network terminal; and

means responsive to receipt of a password entered in response to that request, for writing that received password into the associated respective password store of the newly made entry.

10 5. A method of user authentication in a password protected access system having a password store in which each entry is constituted by a respective user-nominated network terminal identity and an associated respective password, the method comprising the steps of:

in response to receipt at the password protected access system of a call
15 from a calling user at a network terminal, requesting the calling user to enter at that network terminal his nominated terminal identity and password;

receiving the entered terminal identity and password;

accessing the password store in accordance with the received entered terminal identity; and

20 upon locating an entry whose stored network terminal identity and associated password match the received entered terminal identity and password, authenticating that calling user.

6. A method of password update for a password protected access system, the
25 method being as claimed in claim 1 and substantially as hereinbefore described with reference to the drawing.

7. A password protected access system as claimed in claim 2, and
substantially as hereinbefore described with reference to the drawing.

30 8. A method of registering a new user of a password protected access system, the method being as claimed in claim 3 and substantially as hereinbefore described with reference to the drawing.

09.07.2001

G3000

9. A password protected access system as claimed in claim 4, and substantially as hereinbefore described with reference to the drawing.
- 5 10. A method of user authentication in a password protected access system, the method being as claim in claim 5 and substantially as hereinbefore described with reference to the drawing.

Empf.zeit:09/07/2001 18:21

Empf.nr.:156 P.024

AMENDED SHEET

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference A25773 WO	FOR FURTHER ACTION see Notification of Transmittal of International Search Report (Form PCT/ISA/220) as well as, where applicable, item 5 below.	
International application No. PCT/GB 00/ 01010	International filing date (day/month/year) 17/03/2000	(Earliest) Priority Date (day/month/year) 31/03/1999
Applicant BRITISH TELECOMMUNICATIONS PUBLIC LIMITED COMPANY		

This International Search Report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This International Search Report consists of a total of 3 sheets.

☒ It is also accompanied by a copy of each prior art document cited in this report.

1. Basis of the report

a. With regard to the **language**, the international search was carried out on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item.

☐ the international search was carried out on the basis of a translation of the international application furnished to this Authority (Rule 23.1(b)).

b. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international search was carried out on the basis of the sequence listing:

☐ contained in the international application in written form.

☐ filed together with the international application in computer readable form.

☐ furnished subsequently to this Authority in written form.

☐ furnished subsequently to this Authority in computer readable form.

☐ the statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

☐ the statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished

2. ☐ **Certain claims were found unsearchable** (See Box I).

3. ☐ **Unity of Invention is lacking** (see Box II).

4. With regard to the **title**,

☒ the text is approved as submitted by the applicant.

☐ the text has been established by this Authority to read as follows:

5. With regard to the **abstract**,

☒ the text is approved as submitted by the applicant.

☐ the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box III. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. The figure of the **drawings** to be published with the abstract is Figure No.

☒ as suggested by the applicant.

☐ because the applicant failed to suggest a figure.

☐ because this figure better characterizes the invention.

1

☐ None of the figures.

INTERNATIONAL SEARCH REPORT

International Application No

GB 00/01010

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 745 924 A (AT & T CORP) 4 December 1996 (1996-12-04) abstract column 5, line 43 -column 6, line 4 column 7, line 42 -column 8, line 3; figures ----	1-4
X	PATENT ABSTRACTS OF JAPAN vol. 1995, no. 08, 29 September 1995 (1995-09-29) & JP 07 129511 A (NIPPON TELEGR & TELEPH CORP), 19 May 1995 (1995-05-19) abstract ----	1-4
A	EP 0 862 104 A (CASIO COMPUTER CO LTD) 2 September 1998 (1998-09-02) abstract; figures ----- -/--	1-4

☒ Further documents are listed in the continuation of box C.☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search

20 June 2000

Date of mailing of the international search report

28/06/2000

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Moens, R

INTERNATIONAL SEARCH REPORT

International Application No

/GB 00/01010

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 541 435 A (FUJITSU LTD) 12 May 1993 (1993-05-12) abstract -----	1-4

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

/GB 00/01010

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
EP 0745924	A	04-12-1996	US 5721780 A	24-02-1998
			CA 2172566 A	01-12-1996
			JP 8340331 A	24-12-1996

JP 07129511	A	19-05-1995	NONE	

EP 0862104	A	02-09-1998	JP 10243120 A	11-09-1998
			JP 11175477 A	02-07-1999
			CN 1193862 A	23-09-1998

EP 0541435	A	12-05-1993	JP 2000620 C	20-12-1995
			JP 5130096 A	25-05-1993
			JP 7012172 B	08-02-1995
			DE 69202682 D	29-06-1995
			DE 69202682 T	28-09-1995
			KR 9605440 B	25-04-1996
			US 5365580 A	15-11-1994
